

# Exhibit 3

PG.FER.RH-SI-001

27/01/2023

**CODE:** PG.FER.RH-SI-001**TITLE:** PROCEDURE FOR THE USE OF  
TECHNOLOGICAL RESOURCES**VERSION:** 2**SCOPE:** General**LAST REVIEW:** 27/01/2023**CANCELS:** NPRH-0110 of 20 January 2014**DATE OF PUBLICATION:**  
3/2/2023**ORIGINAL VERSION LANGUAGE:** Spanish**APPROVED BY:** Information and Innovation  
Systems Department / Human Resources  
Department**ISSUING AREA:** Information and Innovation Systems  
Department /Human Resources Department**Review history**

Version	Date of Publication	Reason and summary of changes	Cancels/Replaces
1	20/01/2014	Original version	N/A
2	27/01/2023	Updating and adaptation to the new forms of work organization and to the regulatory changes that have been made in this area.	NPRH-0110 of 20 January 2014

## INTRODUCTION

Today, the use and processing of information is mainly carried out with digital resources and supports. It is therefore necessary to establish a series of specific guidelines, complementary to those already included in the Corporate Information Security Framework, relating to the use and control of the information systems and communications networks that process and support Ferrovial's information assets.

Just as is set out in the Corporate Information Security Framework, information is a strategic asset for Ferrovial and, therefore, all the tools necessary for its management must be studied and regulated, so as to ensure that information is handled in accordance with the regulations and best security practices.

Likewise, Ferrovial's values reflected in the Code of Business Ethics imply a commitment to the highest standards of integrity, transparency, respect for the law and human rights. Ferrovial therefore demands that its business be conducted in accordance with these principles and with the utmost respect for applicable national and international laws.

## DEFINITIONS

**Ferrovial:** Ferrovial, S.A. and its subsidiaries, which are understood to be all companies or entities controlled by Ferrovial, S.A. in accordance with article 42 of the Spanish Commercial Code.

**Technological Resources:** are production tools owned by Ferrovial or, failing that, contracted and at the service of Ferrovial, made available to Users so that they can carry out their duties and perform their professional or work duties. The term Technological Resources includes, but without limitation:

- technological infrastructure and services, communications networks, computers, devices, terminals and peripherals that process and treat Ferrovial's information, desktop and/or portable and/or mobile and/or removable and/or for the storage and transport of information, and similar or equivalent mechanisms and elements;
- any information system, application or software program, and similar or equivalent mechanisms and elements;
- Internet services, Intranet, e-mail, instant messaging, collaboration and access services provided by Ferrovial;
- digital identities that give access to the use of hardware and software and, in general, to information systems;
- landlines (e.g. CISCO VoIP), mobile phones and devices (e.g. smartphones and tablets), IoT devices (e.g. wearables), location devices (e.g. tracking, Smart-phones, etc.);
- any other element or technological innovation that Ferrovial currently has or may have in the future;
- professional devices and/or tools that enable the recording of meetings (audio and/or video and/or content) face-to-face or remotely such as telephone terminals (e.g. CISCO VoIP and smartphones), as well as tools and software solutions that facilitate remote meetings (e.g. TEAMS, ZOOM, etc.); and
- access control and security systems and devices.

**Users:** (i) Ferrovial's employees to whom Ferrovial makes Technological Resources available; and (ii) any other person who uses Ferrovial's Technological Resources, even if such use is temporary or occasional, for any reason or circumstance (such as, for example, interns, service providers, consultants, advisers, temporary employment agency personnel, auditors, etc.).

## 1. PURPOSE

The purpose of this procedure is to guarantee that Users make appropriate, responsible and lawful use of the Technological Resources, with the dual purpose of safeguarding the integrity, confidentiality and availability of Ferrovia's information, and to ensure the effective, efficient and secure use and operation of these tools by Users. Ferrovia is also aware of the duty to support Users and wants to ensure that its workplace is a safe environment in which staff can carry out their tasks, without being subject to any threat related to content, inappropriate materials or other improper actions.

## 2. RULES APPLICABLE TO FERROVIA'S TECHNOLOGICAL RESOURCES

The use of Ferrovia's Technological Resources shall be governed by this procedure and by the legislation applicable from time to time, as well as by the provisions of the following "**Related Regulations**" (as amended or replaced in each case): (i) the Code of Business Ethics, (ii) the Corporate Information Security Framework, (iii) the Information Security Roles and Responsibilities document, (iv) the Corporate Cybersecurity Policy, (v) the Confidential Information Classification and Processing Regulation, (vi) the Policy for the Elimination and Conservation of Electronic Mail, Instant Messages and Calendar Appointments and, where applicable, (vii) the specific internal regulations for the use of certain Technological Resources and the processing of Ferrovia information. Users must also take into account the Decalogue for the Processing of Confidential Information in the use of Ferrovia's Technological Resources.

## 3. SCOPE OF APPLICATION

This procedure is applicable to Users subject to any of the legal systems mentioned in Annex 1.

## 4. NATURE AND USE OF THE TECHNOLOGICAL RESOURCES

### 4.1 NATURE OF TECHNOLOGICAL RESOURCES

Technological Resources are a key asset of Ferrovia and should be considered production tools at the service of its businesses and activities. Technological Resources are made available to Users for the purpose of fulfilling the specific obligations of their job in accordance with the rules of good faith and diligence.

### 4.2 USE OF TECHNOLOGICAL RESOURCES

The improper use of Technological Resources may generate damages for Ferrovia that may be extremely serious, including the imputation of criminal liability to Ferrovia for criminal offences committed by individuals within its organisation, unless it can be shown that due control has been exercised over them. Ferrovia has a legitimate interest in protecting its business activities, reputation, resources and equipment and in ensuring a safe workplace for Users and other employees.

### 4.3 PROHIBITIONS

It is expressly forbidden to use the Technological Resources in violation of the employment contract or any conduct punishable under the applicable labour regulations, as well as, in general, any use that constitutes a breach of the legislation in force. Any practices contrary to this procedure and the Related Regulations are also prohibited.

In particular, and without limitation, it is forbidden to use any Technological Resources for the purpose or as a result of:

- committing criminal offences, regardless of whether a benefit is sought or obtained for Ferrovia;
- harassing or discriminating;

- disclosing confidential information, unless expressly authorised to do so, or failing to comply with personal data protection regulations;
- undermining the security of Ferrovial and its tangible and intangible assets (ownership of property, intellectual and industrial property rights, goodwill, reputation, good image, etc.);
- jeopardising the security and stability of the Technological Resources or the information contained therein, among other things, by not informing the Information Systems and Innovation Department of any suspicion of doubt or weak point therein;
- committing acts of unfair competition against Ferrovial;
- violating other rights of Ferrovial or third parties;
- breaching of contracts or relations between Ferrovial and Users, including the dedication of work time to leisure and other activities unrelated to the relationship with the company, and the lack of an adequate level of performance at work as a consequence of such inappropriate use;
- engaging in any other conduct contrary to the legal system, the regulations in force or good contractual faith within the company. Producing, transmitting, distributing, storing, downloading, installing, copying, displaying, sending, requesting or receiving any kind of offensive, pornographic or discriminatory content, especially if its possession or use constitutes an illegal action. This includes, without limitation, any copyrighted material, trademarks, trade marks, trade secrets or other intellectual or industrial property rights used without proper authorisation;
- intentionally deleting or destroying Ferrovial information supported and/or processed by the Technological Resources, unless expressly authorised;
- disabling, frustrating or circumventing any security measures deployed to safeguard Ferrovial's Technological Resources or information;
- accessing or using Ferrovial's Technological Resources, or the information supported and/or processed by them, when they do not have authorisation to do so;
- intentionally transmitting or downloading malicious software (malware) or similar via the Technology Media (e.g. viruses);
- downloading, distributing, sending or installing any software without the express authorisation of the Information Systems and Innovation Department;
- obtaining information relating to access identifiers and digital identity authentication mechanisms assigned to other Users, unless expressly authorised or in the exercise of the functions of a User at the service of Ferrovial;
- hiding the User's digital identity, impersonating the User or pretending to belong to an organisation other than Ferrovial;
- downloading and/or storing confidential, sensitive or personal information on Technology Resources not adequately configured to protect such information;
- incurring, through the use of the Technological Resources, expenses that have not been previously authorised, or that are unnecessary, excessive or disproportionate in view of the purpose of their use; and

- modifying the configuration of the Technological Resources or accessing it without the knowledge and authorisation of the Information Systems and Innovation Department.

## 5. CONTROL OF TECHNOLOGICAL RESOURCES

Insofar as they are work tools, the Technological Resources are made available to Users so that they may use them to prepare, transmit, distribute, store, download, install, copy, view, send or receive content specific to their professional activity and for the proper performance of their work at the service of Ferrovia.

It should also be borne in mind that, in accordance with the applicable rules, and in accordance with the principles of proportionality, reasonableness and appropriateness:

- Ferrovia has the right to supervise, control and monitor that the Technological Resources are used in accordance with the provisions of this procedure, the Related Regulations and other applicable laws and regulations; and
- Ferrovia has a duty to prevent the commission of criminal offences within its organisation, to provide its employees with a safe workplace, and to protect its own resources.

Therefore, Users should be aware that there is no expectation of privacy, confidentiality or secrecy of communications or information created, received, stored or transmitted using Ferrovia's Technological Resources.<sup>1</sup>

All information and communications stored or transmitted using the Technological Resources are the property of Ferrovia and may be retained by Ferrovia for the applicable periods of time in accordance with the regulations in force at any given time.

Ferrovia may access, control and monitor all Technological Resources, always in accordance with applicable law and respecting the principles of proportionality, rationality and suitability, in order to:

- verify compliance with the provisions of this procedure, the contract between the User and Ferrovia, and the applicable regulations;
- ensure that Users do not commit criminal offences and thus demonstrate that due control has been exercised;
- guarantee a secure workplace for Users;
- check the proper application by the Users of the security and use measures and procedures established by Ferrovia;
- sanction or take legal action against Users and other workers who engage in prohibited conduct and being able to prove such conduct before judicial or other authorities; and
- respond to requests issued by judicial bodies or other public authorities, in accordance with the legal limits and requirements applicable at any given time.

## 6. SAFETY REGULATIONS

The following regulations shall apply in order to preserve and protect the Technological Resources and the information processed through them.

<sup>1</sup> The non-existence of an expectation of privacy, confidentiality or secrecy of communications shall in no case affect the information communicated to Ferrovia through the Ethical Channel, in which context Ferrovia guarantees the confidentiality of the identity of the informant and of any third party mentioned in the communication sent, as well as of the actions carried out during the management and processing of said communication.

## 6.1 ACCESS

Unless otherwise established or not appropriate due to the nature of the resource in question, access to Ferrovia's Technological Resources by Users shall require a personal access identifier (User code) accompanied by a mechanism for authenticating their identity (for example, a password).

The assignment to Users of access identifiers to the Technological Resources shall be carried out by the Human Resources and Information Systems and Innovation Departments.

The access identifiers provided to each User shall be personal, secret and non-transferable; they shall be protected and shall under no circumstances be shared.

It is the responsibility of Users to maintain the utmost discretion and confidentiality of their identity authentication mechanisms in order to avoid unauthorised disclosure and use.

Users shall be responsible for all actions carried out with their access identifier, except in cases of fraudulent impersonation.

## 6.2 CONFIGURATION AND CUSTODY

The configuration of Technological Resources is the responsibility of the Information Systems and Innovation Department, which shall deploy the appropriate security mechanisms and controls to reduce the risk of information leakage and/or theft, unauthorised access and loss of integrity and availability of Ferrovia's information.

Users of Technology Resources shall be responsible for preventing unauthorised or improper access to them.

Users of portable / mobile / removable Technology Resources shall at all times avoid leaving them unattended. In addition, they shall ensure the safekeeping of these when they are not in use.

For security reasons, only removable storage and transport devices that guarantee the confidentiality and integrity of the information contained therein and incorporate appropriate protection measures may be used.

Also for security reasons, Users should, as far as possible, avoid storing sensitive information on local drives at workstations. To this end, the User shall store the sensitive information generated in the repositories and storage services provided by the Information Systems and Innovation Department (e.g. TEAMS, ONEDRIVE, SHAREPOINT, etc.).

Users shall limit access to and distribution of sensitive information to a restricted, duly authorised and need-to-know group.

Given that storage capacity is limited, each User shall be responsible for deleting duplicate or obsolete information, in compliance with existing applicable information deletion and retention regulations.

Printouts of Ferrovia information made by Users on devices such as printers, scanners, photocopiers, etc. must be made using secure means, they must not be left unattended and must be collected as quickly as possible.

Whenever Technological Resources leave Ferrovia's premises, Users must comply with the security guidelines established for such cases.

## 6.3 INSTALLATION OF SOFTWARE AND/OR HARDWARE

The installation of software and/or hardware on the Technological Resources is not permitted without the express authorisation of the Information Systems and Innovation Department.

## 6.4 COMMUNICATIONS

The configuration of Ferrovial's communications infrastructure is the responsibility of the Information Systems and Innovation Department, which shall deploy the appropriate security mechanisms and controls to guarantee the integrity, confidentiality and availability of the information transmitted through it.

It is not permitted to connect Ferrovial's Technological Resources to external communications infrastructures and networks without the authorisation of the Information Systems and Innovation Department. Likewise, it is not permitted to connect the tools and/or solutions and/or devices of third parties to Ferrovial's networks without prior authorisation.

## 6.5 USE OF E-MAIL (INCLUDING CORPORATE INSTANT MESSAGING APPLICATION) AND INTERNET/INTRANET ACCESS

Email (which includes the corporate instant messaging application available at any given time and the rest of the collaboration and information storage and backup solutions, such as the Microsoft 365 suite) and internet/intranet access are currently two of the most useful tools for Users to access and transmit information in the performance of their duties.

The use of e-mail (which includes the corporate instant messaging application) and Internet/Intranet Access shall comply with the regulations and principles set out in this section.

Caution should be exercised both when sending information and when selecting the recipients of the information, as information sent via e-mail and/or internet/intranet can be read, copied or retransmitted by the recipient, with the particularity that the communication usually contains sufficient information to identify the initial sender and the corporate environment from which it was sent.

In order to avoid malware infections through the use of e-mail and internet/intranet, you should not download and/or install and/or execute files of unknown origin and/or without proper authorisation, even if you have verified that they do not contain malware.

Extreme caution should be exercised when opening and reading messages received by e-mail and/or SMS from unknown senders, especially when accessing links, opening attachments and/or content included therein.

E-mail is an information exchange tool and not a storage tool. The information that needs to be kept shall be archived in the repositories and storage services enabled by the Information Systems and Innovation Department for this purpose (e.g. TEAMS, ONEDRIVE, SHAREPOINT, etc.), and the rest shall be deleted, unless its preservation is duly authorised. The User must follow the indications included in the Policy for the Elimination and Conservation of E-mails, Instant Messages and Calendar Appointments for the conservation and storage of the information contained in the e-mail.

For security reasons, unless duly authorised by the Information Systems and Innovation Department, the systematic forwarding of messages received in corporate e-mail accounts to e-mail accounts not provided by Ferrovial is not permitted, nor vice versa, nor is the automatic forwarding of messages received in non-Ferrovial e-mail accounts to corporate e-mail accounts.

Communications with content of a general nature or that may be of interest to large groups of people should be channelled through other information, communication, collaboration or dissemination tools established for such purposes (e.g. circulars, news, announcements, etc. on the corporate intranet, Microsoft 365 tools, employee portals, etc.), and not through e-mail messages.

The use of e-mail distribution lists for the dissemination of information to specific groups of people should be subject to the following guidelines:

- They shall only be used for the dissemination of information related to Ferrovial's own activities.
- They should not be used indiscriminately, as too much information can be as negative as too little.



- Messages to distribution lists should avoid including large attachments (larger in total than 10 MB).
- The use of electronic mail for the distribution or propagation of "chain letters", pyramid schemes or other such electronic messages is expressly prohibited.

In order to avoid the degradation of the corporate e-mail service and the saturation of Users' mailboxes, instead of attaching files in the messages to be sent, the inclusion of links to the repositories where they are stored (TEAMS, ONEDRIVE, SHAREPOINT, etc.) should be considered. If this is not possible or desirable for any reason, compression of large files should be considered before attaching them to a message (the same rule applies when attaching a large number of files if they are collectively very large). As a general rule, files with a total size of more than 10 MB should not be attached to an e-mail.

Ferrovial reserves the right to block access to certain internet/intranet pages at any time and without prior notice. In particular, it may block access to those addresses whose content or level of security does not comply with the principles and regulations contained in the Related Regulations and, in particular, in the Corporate Information Security Framework and in this procedure. The corporate email should include the corporate confidentiality notice model.

Without prejudice to the provisions of section 5 above, Ferrovial may access the User's corporate email account (as well as the company's instant messaging application), in accordance with the principles of proportionality, reasonableness and suitability, when the User is on holiday or unable to perform their duties due to illness or absence. In such cases, the following conditions must be met for the opening of e-mails and messages:

- such opening shall only be carried out to ensure the continuity of the business, and exclusively in relation to Users who are Ferrovial employees; and
- an attempt shall be made to inform the person concerned in advance. If this is not possible, the employee shall be informed subsequently, as soon as practicable, and the opening of business mails and messages shall take place in the physical or virtual presence of the employee's line manager and after assessment by the latter of the need for intervention for business continuity.

Exceptionally, and in case of extreme necessity (for example, because the e-mail service is not available and communication is urgent and necessary), the User may use their private e-mail accounts to carry out their professional or work duties. In the event that its use is essential, the User's Ferrovial e-mail address must be copied and it shall be understood that the User authorises the company to access the content of said e-mails used for professional or work-related purposes, in accordance with the principles of proportionality, reasonableness and suitability.

## **7. REPORTING OF INCIDENTS IN THE USE OF TECHNOLOGICAL RESOURCES**

The User must notify the Cybersecurity Division of the Information and Innovation Systems Department and/or the User Service Centre, with the utmost urgency and by the means established for this purpose, of any incident that may involve a breach of the confidentiality and/or integrity and/or availability of the Technological Resources (for example, the theft or loss of any device or the detection of malware).

## **8. RETURN AND CESSATION OF THE USE OF TECHNOLOGICAL RESOURCES**

In the event of termination of the User's relationship with Ferrovial for any reason, the User is obliged to return or cease to use, as appropriate, the Technological Resources made available to them. To this end, Ferrovial shall terminate and disable access to the Technological Resources in question.

In cases of suspension of the relationship (for example, due to temporary disability, leave of absence, etc.), Ferrovial may require the User to return or cease using Ferrovial's Technological Resources.

## **9. RECORDINGS OF MEETINGS USING TECHNOLOGICAL RESOURCES**

The recording of meetings, conversations and/or their contents held in the work or professional environment through the use of Technological Resources constitutes a personal data processing activity to which Regulation (EU) 679/2016, General Data Protection Regulation and Organic Law 3/2018, on the Protection of Personal Data and Guarantee of Digital Rights, are applicable.

The recording of meetings and conversations with the User's own and private means is prohibited, and may only be carried out with the Technological Resources if one of the following conditions is met:

- that the recording is made in the context of a training action and for the purpose of reusing it at a later date for re-delivery to Ferrovial employees. Participants shall be informed prior to the meeting or conversation that it shall be recorded for this purpose; or
- the express consent of all participants to the recording has been obtained prior to the recording. In such a case, appropriate evidence of having obtained such consent shall be kept.

Template texts and/or voiceovers to inform about the recording and to obtain the above-mentioned consent are provided in Annex 2.

\* \* \* \*

**ANNEX 1**

This procedure has been validated in the countries mentioned below:

- Canada (Ontario)
- Chile
- U.S, (Texas, New York, California and Virginia)
- Spain
- Ireland
- Puerto Rico
- United Kingdom

**ANNEX 2**

This Annex sets out the informative clauses that Users must include in the notice of a meeting that is to be recorded. In any case, these are models that must be adapted by the User according to the circumstances of each case.

If the informative clauses are used in cases in which the RGPD is not applicable, they must be previously adapted to the applicable legislation in the corresponding jurisdiction.

**A. Information clause in english and spanish for recording training sessions**

By means of this e-mail and in compliance with data protection regulations, we inform you that the [area/department of \_\_\_\_\_] will record the training session in which you may participate and in which your image and voice may be recorded ("**Training**").

Your data will be processed by \_\_\_\_\_<sup>2</sup> ("**Ferrovial**"), as the data controller, in order to enable the development, monitoring and subsequent reproduction of the training session. The legitimacy of such data processing is based on Ferrovial's legitimate interest in ensuring the participation of employees who cannot attend the training sessions live.

Please note that you can exercise your rights of access, rectification, deletion, opposition, limitation of processing, right to portability or that your data are not subject to automated individual decisions by sending an email to the Data Protection Officer ([dpd@ferrovial.com](mailto:dpd@ferrovial.com))<sup>3</sup>. You can also exercise your rights before the competent data protection supervisory authority.

The data will be kept until (i) the intended purpose is fulfilled or (ii) the data subject requests said data to be deleted or withdraws the consent. The collected data will not be disclosed to third parties, unless legally required.

—

Mediante el presente correo electrónico y en cumplimiento de la normativa de protección de datos, le informamos que el [área/departamento de \_\_\_\_\_] va a grabar la sesión de formación en la que usted podrá participar y en la que se podrá captar su imagen y su voz ( la "**Formación**").

Sus datos serán tratados por \_\_\_\_\_<sup>4</sup> ("**Ferrovial**"), como responsable del tratamiento, con la finalidad de posibilitar el desarrollo, seguimiento y reproducción posterior de la formación impartida en dicha sesión. La legitimación de dicho tratamiento de datos se basa en el interés legítimo de Ferrovial en garantizar la participación de los empleados que no puedan asistir a las sesiones formativas en directo.

Le informamos de que puede ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, derecho a la portabilidad o a que sus datos no sean objeto de decisiones individuales automatizadas enviando un correo al Delegado de Protección de Datos ([dpd@ferrovial.com](mailto:dpd@ferrovial.com))<sup>5</sup>. También puede ejercitar sus derechos ante la autoridad de control competente en materia de protección de datos.

Los datos serán conservados (i) hasta alcanzar la finalidad perseguida o (ii) hasta que el interesado solicite su supresión o retire su consentimiento. Los datos que se recaben no serán comunicados a terceros, salvo en cumplimiento de una obligación legal.

<sup>2</sup> The User that organizes the training session shall complete this section with the name of the company that the User belongs to.

<sup>3</sup> Users belonging to a Ferrovial entity which is not subject to Spanish law shall contact the Data Protection Office, which will adapt this paragraph.

<sup>4</sup> El Usuario organizador de la reunión debe completar este apartado con la denominación de la sociedad a la que pertenece el área/departamento que organiza la formación.

<sup>5</sup> Los Usuarios que pertenezcan a una entidad de Ferrovial no sujeta a la legislación española deberán contactar con la Oficina de Protección de Datos, que se ocupará de adaptar este párrafo.

**B. Information clause in english and spanish for recording sessions for other purposes**

By means of this e-mail and in compliance with data protection regulations, we inform you that the [area/department of \_\_\_\_\_] will record a session or meeting in which you are invited to participate, where your image and voice may be recorded (the "**Initiative**").

Your data will be processed by \_\_\_\_\_<sup>6</sup> ("**Ferrovial**"), as the data controller, for the purpose of \_\_\_\_\_<sup>7</sup>.

Please note that you can exercise your rights of access, rectification, deletion, opposition, limitation of processing, right to portability or that your data are not subject to automated individual decisions by sending an email to the Data Protection Officer ([dpp@ferrovial.com](mailto:dpp@ferrovial.com))<sup>8</sup>. You can also exercise your rights before the competent data protection supervisory authority.

The data will be kept until (i) the intended purpose is fulfilled or (ii) the data subject requests said data to be deleted or withdraws the consent. The collected data will not be disclosed to third parties, unless legally required.

The legitimacy of such data processing is based on your consent. Please reply to this e-mail and confirm that you consent to the processing of your image and voice by Ferrovial in accordance with the provisions of this informative e-mail.

—

Mediante el presente correo electrónico y en cumplimiento de la normativa de protección de datos, le informamos que el [área/departamento de \_\_\_\_\_] va a proceder a la grabación de una sesión o reunión a la que usted está siendo convocado y en la que se podrá captar su imagen y su voz (la "**Iniciativa**").

Sus datos serán tratados por \_\_\_\_\_<sup>9</sup> ("**Ferrovial**"), como responsable del tratamiento con la finalidad de \_\_\_\_\_<sup>10</sup>.

Le informamos de que puede ejercitar sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, derecho a la portabilidad o a que sus datos no sean objeto de decisiones individuales automatizadas enviando un correo al Delegado de Protección de Datos ([dpp@ferrovial.com](mailto:dpp@ferrovial.com))<sup>11</sup>. También puede ejercitar sus derechos ante la autoridad de control competente en materia de protección de datos.

Los datos serán conservados (i) hasta alcanzar la finalidad perseguida o (ii) hasta que el interesado solicite su supresión o retire su consentimiento. Los datos que se recaben no serán comunicados a terceros, salvo en cumplimiento de una obligación legal.

La legitimación de dicho tratamiento de datos se basa en su consentimiento. Le rogamos que por favor responda a este correo electrónico y confirme que consiente que su imagen y voz sean tratadas por Ferrovial según lo previsto en este correo informativo.

<sup>6</sup> The User that organizes the meeting shall complete this section with the name of the company that the department belongs to.

<sup>7</sup> The User that organizes the meeting intended to be recorded shall include in this section the specific purpose of the recording.

<sup>8</sup> Users belonging to a Ferrovial entity which is not subject to Spanish law shall contact the Data Protection Office, which will adapt this paragraph.

<sup>9</sup> El Usuario organizador de la reunión debe completar este apartado con la denominación de la sociedad a la que pertenece su área/departamento.

<sup>10</sup> El Usuario organizador de la reunión que se propone grabar deberá incluir en este apartado la finalidad concreta de la grabación.

<sup>11</sup> Los Usuarios que pertenezcan a una entidad de Ferrovial no sujeta a la legislación española deberán contactar con la Oficina de Protección de Datos, que se ocupará de adaptar este párrafo.